IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Christian Gehrmann et al.	§	Group Art Unit:	2136
Serial No:	09/692,709	§	Examiner:	Hoffman, Brandon
Filed:	October 19, 2000	§	Confirmation No:	7545

Attorney Docket No: P12266/45687-00036
Customer No.: 27045

For: Method and Arrangement in a Communication Network

Via EFS-Web

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313.1450

CERTIFICATE OF TRANSMISSION BY EFS-WEB

Date of Transmission: July 24, 2006

I hereby certify that this paper or fee is being transmitted to the United States Patent and Trademark Office electronically via EFS-Web.

Type or Print Name: Pamela C. Shultz

Pamela C Shultz

APPEAL UNDER 35 U.S.C. §134

This Brief is submitted in connection with the decision of the Primary Examiner set forth in Final Official Action dated March 29, 2006 (Paper No. (not identified)), finally rejecting Claims 1 and 4-23, which are all of the pending claims in this application.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §41.20(b)(2) that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1379.

Real Party in Interest

The real party in interest, by assignment, is: Telefonaktiebolaget LM Ericsson (publ)
SE-164 83
Stockholm, Sweden

Related Appeals and Interferences

None.

Status of Claims

Claims 1 and 4-23 are pending in the present application, each of which are finally rejected and form the basis for this Appeal. Claims 1, 4-6 and 17-18, stand rejected, under 35 U.S.C. §103(a), as being unpatentable over "Merging and Extending the PDP and PEM Trust Models – The ICE-TEL Trust Model", Chadwick et al., May/June 1997 (hereinafter referred to as Chadwick) in view of Hunt el al. (US 5,539,881); and Claims 7-16 and 19-23 stand rejected as being unpatentable over Chadwick in view of Hunt and further in view of Morris et al. (US 6,691,173). Claims 1 and 4-23, including all amendments to the claims, are attached in the Claims Appendix. The rejection of Claims 1 and 4-23 is appealed.

Status of Amendments

The claims set out in the Claims Appendix include all entered amendments. No amendment has been filed subsequent to the final rejection.

Summary of Claimed Subject Matter

Claim Element	Specification Reference
at least two nodes (103-105) of the set of communication nodes (101, 103-105) having a mutual trust relation and comprising a trust group (102), the trust relations being created with public keys	Page 5, lines 8-9 Page 6, lines 27-30 Figure 1 (as indicated) Figures 2-6 and the associated text provide additional examples
at least one additional node (101), the at least one additional node (10) being a candidate node for joining the trust group (102) within the ad hoc communication network (106)	Page 5, lines 9-10 Page 7, lines 9-11 Figure 1 (as indicated) Figures 2-6 and the associated text provide additional examples

the nodes having authority to delegate trust to nodes of the set of communication nodes (103-105) within the trust group (102)	Page 7, lines 1-5 Figure 1 (as indicated) Figures 2-6 and the associated text provide additional examples
receiving a request from the candidate node (101) to join the trust group (102) within said ad hoc communication network (106) wherein said ad hoc communication network (106) does not include a separate certificate authority	Page 7, lines 9-17 Figure 1 (as indicated) Figures 2-6 and the associated text provide additional examples
identifying any node (103) within the trust group (102) having a trust relation with the candidate node (101), the node having the trust relation with the candidate node (101) being an X-node (103)	Page 5, lines 10-12 Page 7, lines 19-20 Figure 1 (as indicated) Figures 2-6 and the associated text provide additional examples
distributing trust relations between all members in the trust group (102) and the candidate node (101) by means of the X-node (103) distributing the public key associated with said candidate node (101) to said all members of the trust group (102) and wherein X-node (103) further sending a signed message comprising a list of nodes (104-105) that the X-node (103) trusts within the ad hoc communication network (106) and all corresponding public keys to the candidate node (101)	Page 5, lines 12-13 Page 7, lines 19-25 Page 8, lines 4-9 Figure 1 (as indicated) Figures 2-6 and the associated text provide additional examples

The specification references listed above are provided solely to comply with the USPTO's current regulations regarding appeal briefs. The use of such references

should not be interpreted to limit the scope of the claims to such references, nor to limit the scope of the claimed invention in any manner.

Grounds of Rejection to be Reviewed on Appeal

1.) Claims 1, 4-6 and 17-18 stand rejected, under 35 U.S.C. §103(a), as being unpatentable over "Merging and Extending the PDP and PEM Trust Models – The ICE-TEL Trust Model", Chadwick et al., May/June 1997 in view of Hunt el al. (US 5,539,881).

2.) Claims 7-16 and 19-23 stand rejected, under Chadwick et al. in view of Hunt et al. and further in view of Morris et al. (US 6,691,173).

Argument

1.) Rejection under 35 U.S.C. 103(a) over "Merging and Extending the PDP and PEM Trust Models – The ICE-TEL Trust Model" in view of United States Patent No. 5,539,881

In order to establish a prima facie case of obviousness, three criteria must be met: (1) there must be some suggestion or motivation in the prior art to modify the reference or to combine reference teachings as proposed, (2) there must be a reasonable expectation of success, and (3) the prior art or combined references must teach or suggest all the claim limitations. MPEP § 2143; In re Vacek, 947 F.2d 488 (Fed. Cir. 1991). "The prior art must suggest the desirability of the claimed invention." MPEP § 2143.01. Both the invention and the prior art references must be considered as a whole. MPEP § 2141.02. The Applicant respectfully submits that claims 1 and 17 are not obvious over the cited art and are, therefore, allowable under 35 U.S.C. § 103(a) for the reasons stated below.

Claims 1 and 17

The Chadwick Reference was incorrectly applied to Claims 1 and 17

The Chadwick reference discloses a method in which a user determines who he/she will trust by storing the public keys of trusted entities in his/her personal security environment (PSE). (page 24, left column). The user can also delegate the trust determination to the security administrator of his/her certification authority. (page 24, left column). Although the user can keep its own list of trusted entities (page 19, "Personal Security Environment"), the user cannot add a candidate entity to (a) another user's list of trusted entities (Id.; page 24, left column) or (b) a trusted group of users that is larger than the user itself (page 19, "Trusted Point"; page 22, left column). Adding a candidate entity to a trusted group of users that is larger than a single user can only be done through the certification authority responsible for that trusted group. (page 19, "Trusted Point").

A user can decide whether or not to trust a message received from another user without having the other user's public key stored in his/her personal security environment (PSE) if the message contains a certification path for the other user. (page 20, "Certification Path"). The certification path contains a sequence of signed and interlinked certificates starting with a certificate signed by a certification authority and ends with the certificate of the other user. Id. The user receiving the message will trust the public key from the other user when the certification path contains one or more certificates signed by a certification authority trusted by the user. Id.

The Chadwick reference discloses an example where User 1 (a member of trust groups OrigCA and PCA1) decides to trust his/her trust point certification authority (PCA1) and User 4 (not a member of any security domain) by manually entering the public keys for PCA1 and User 4 into User 1's personal security environment (PSE). (page 22, left column, first paragraph). Thereafter, messages containing the signature of User 4 can be immediately verified and trusted based on the contents of User 1's PSE. (page 22, left column, second paragraph). User 4 is not trusted by trust group OrigCA or PCA1. User 4 is only trusted by User 1. User 1's trust of User 4 is not

communicated, passed or delegated to any other entity. As a result, User 4 does not join and is not a candidate to join the trust group OrigCA or PCA1 of which User 1 is a member. Note that User 2 and User 3 are not candidate nodes for joining trust group OrigCA or PCA1 because messages from User 2 will be trusted by User 1 (cross-certificate between PCA1 and PCA2) and messages from User 3 will not be trusted by User 1 (no cross-certificate between PCA1 and PCA3).

The Applicant respectfully submits that the Chadwick reference was incorrectly applied to Claims 1 and 17 for the following reasons:

First, the Examiner incorrectly interpreted the Chadwick reference to disclose "receiving a request from the candidate node to join the trust group within said ad hoc communication network wherein said ad hoc communication network does not include a separate certificate authority." (Final Official Action dated March 29, 2006, page 3, lines 9-14). As recited in Claims 1 and 17, a "trust group" comprises "at least two nodes of the set of communication nodes having a mutual trust relation". (Claim 1, lines 2-4; Claim 17, lines 6-7). As a result, a single user cannot be a trust group. The Applicant respectfully submits that the single user security domains described in the Chadwick reference do not disclose, teach or suggest "receiving a request from the candidate node to join the trust group within said ad hoc communication network wherein said ad hoc communication network does not include a separate certificate authority" because the trust group comprises at least two nodes. In addition, the Applicant respectfully submits that the Chadwick reference do not disclose, teach or suggest "receiving a request from the candidate node to join the trust group within said ad hoc communication network wherein said ad hoc communication network does not include a separate certificate authority" because the multiple user security domains or trust groups described in the Chadwick reference always include a separate certificate authority. (Figures 1-4). As a result, the Chadwick reference was incorrectly applied to Claims 1 and 17.

Second, the Examiner incorrectly interpreted the Chadwick reference to disclose "identifying any node within the trust group having a trust relation with the candidate node, the node having the trust relation with the candidate node being an X-node." (Final Official Action dated March 29, 2006, page 3, lines 15-17). The Examiner

identified the discussion of "Cross Certification" in the Chadwick reference to support his interpretation. The Applicant respectfully submits that the cited portions of the Chadwick reference do not disclose, teach or suggest "identifying any node within the trust group having a trust relation with the candidate node, the node having the trust relation with the candidate node being an X-node" because the "Cross Certification" process is always conducted between two certification authorities. (page 20, right column). Claims 1 and 17 recite that the trust group comprises at least two nodes and the "ad hoc communication network does not include a separate certificate authority". As a result, "any node within the trust group" cannot be a single user security domain or a certificate authority. As a result, the Chadwick reference was incorrectly applied to Claims 1 and 17.

Third, the Examiner incorrectly interpreted the Chadwick reference to disclose "wherein X-node further sending a signed message comprising a list of nodes that the X-node trusts within the ad hoc communication network and all corresponding public keys to the candidate node." (Final Official Action dated March 29, 2006, page 3, lines 18-21). The Examiner identified the discussion of "Cross Certification" in the Chadwick reference to support his interpretation. The Applicant respectfully submits that the cited portions of the Chadwick reference do not disclose, teach or suggest "wherein X-node further sending a signed message comprising a list of nodes that the X-node trusts within the ad hoc communication network and all corresponding public keys to the candidate node" because the "Cross Certification" process is always conducted between two certification authorities. (page 20, right column). Claims 1 and 17 recite that the trust group comprises at least two nodes and the "ad hoc communication network does not include a separate certificate authority". As a result, "any node within the trust group" cannot be a single user security domain or a certificate authority. In addition, the "Cross Certification" process does not send a list of all nodes trusted by the X-node along with all the corresponding keys to the candidate node. Only the keys of the respective certification authorities are exchanged. (page 20, "Cross Certification"). A list of nodes and the corresponding security key of the nodes within the respective security domains are not exchanged. Id. As a result, the Chadwick reference was incorrectly applied to Claims 1 and 17.

The Examiner acknowledged that the Chadwick reference does not does not teach "distributing trust relationships between all members in the trust group and the candidate node by means of the x-node distributing the public key associated with said candidate node to said all members of the trust group." (Final Official Action dated March 29, 2006, page 4, lines 1-3).

The Hunt Reference was incorrectly applied to Claims 1 and 17

The Hunt reference discloses the use of a Directory Services Network Element (DSNE) to store and update identity information for all elements within a network. (col. 1, lines 41-47, 61-67). Storing the identity information at the DSNE solved the stated problem of having the identity information for all network elements stored at each network element (col. 1, lines 22-32). As a result, each element in the network does not have to store identity information about all elements in the network. A new network element registers its identity information with the DSNE. (col. 1, lines 57-64). Once registered, the new network element can communicate with the DSNE to obtain information about other elements in the network so that the new network element can communicate with them. (col. 1, line 64-col. 2, line 3).

The DSNE stores the identity information along with a SONET Management Sub-system Branch (SMSB) update flag in a directory information base (DIB). (Figures 10, 18 and associated text). When the identity information for an element within a specified SMSB is added, changed or deleted, the SMSB update flag will cause the DSNE to send the updated identity information to the other elements within the specified SMSB. (Figure 7 and associated text). So, the elements within a specified SMSB only contain identity information for the DSNE and the other elements with the specified SMSB. (Figures 11-13, 19-24 and associated text). The DSNE is, therefore, the only element that "distributes" identity information in the network. The other network elements do not exchange identity information with one another.

The Applicant respectfully submits that the Hunt reference was incorrectly applied to Claims 1 and 17 for the following reasons:

First, the Examiner incorrectly interpreted the Hunt reference to teach that more than one node performs the functions of the DSNE or X-node at any given time. (Final Official Action dated March 29, 2006, page 9, lines 4-7). In response to the Applicant's argument traversing the Examiner's rejection, the Examiner further stated that:

> "Hunt et al. teaches, on column 3, lines 16-20 that network element 100 may be either a DSNE or a remote NE. This means that any network element has the opportunity to become the DSNE, or X-node."

(Final Official Action dated March 29, 2006, page 9, lines 4-7). The cited portion of the Hunt reference merely states that a DSNE network element (100) can be employed as either a DSNE or a remote Network Element (NE) in a telecommunications management network. However, whether deployed as a local NE or a remote NE, only the identity of this particular DNSE network element is then supplied to each newly reachable network element as it is added to the network (col. 1, lines 49-64). Accordingly, it is not "any node within the trust group having a trust relation with the candidate node" that is being identified as an "X-node" in accordance with the teachings of the present invention. Instead, a particular network element (whether local or remote) is first identified as the DSNE in the Hunt reference and it is the identity of this pre-designated DSNE that is provided to a newly reachable network element that is being added to the network. As a result, the Hunt reference was incorrectly applied to Claims 1 and 17.

Second, the Examiner incorrectly interpreted the Hunt reference to teach "the remote NE (candidate node) receives information from other nodes and transmits its information to other nodes." (Final Official Action dated March 29, 2006, page 9, lines 12-13). However, as clearly recited in the present application, it is the "X-node" and not the candidate node that distributes the public key associated the candidate node to all other members of the trust group. Furthermore, it is the X-node and not the candidate node that further sends a signed message comprising a list of all trusted nodes and corresponding public keys to the candidate node. Accordingly, even based on the Examiner's own understanding of the Hunt reference, the present invention is different and distinguishable from the Hunt reference. As a result, the Hunt reference was incorrectly applied to Claims 1 and 17.

There is no teaching or suggestion in the prior art to modify the reference as proposed.

Obviousness can only be found where there is some teaching, suggestion, or motivation to modify a reference in the manner proposed, found either in the prior art itself or in the knowledge generally available in the art. See MPEP § 2143.01; In re Fine, 837 F.2d 1071 (Fed. Cir. 1988); In re Jones, 958 F.2d 347 (Fed. Cir. 1992). In addition, obviousness can only be found under a combination of references where there is some teaching, suggestion, or motivation to do so, found either in the references themselves or in the knowledge generally available in the art. Id. Further, the mere fact that references can be combined or modified does not necessarily make the combination obvious unless the prior art suggests the combination. See MPEP § 2143.01; In re Mills, 916 F.2d 680 (Fed. Cir. 1990). Finally, simply stating that a claimed modification of the prior art would have been "obvious to a person of ordinary skill in the art at the time the invention was made" because all aspects of the claimed invention were individually known in the art is not enough to establish a prima facie case of obviousness without some objective reason to combine the teachings. MPEP § 2143.01; Ex parte Levengood, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993).

For the reasons stated above, the cited references provide separate and distinct systems that contain numerous deficiencies when correctly applied to Claims 1 and 17. The cited references do not provide any teaching or suggestion to modify themselves to correct the numerous deficiencies. More specifically, there is no teaching or suggestion to modify the Chadwick reference or the Hunt reference to:

> receiving a request from the candidate node to join the trust group within said ad hoc communication network wherein said ad hoc communication network does not include a separate certificate authority;
>
> identifying any node within the trust group having a trust relation with the candidate node, the node having the trust relation with the candidate node being an X-node; and

distributing trust relations between all members in the trust group and the candidate node by means of the X-node distributing the public key associated with said candidate node to said all members of the trust group and wherein X-node further sending a signed message comprising a list of nodes that the X-node trusts within the ad hoc communication network and all corresponding public keys to the candidate node.

Moreover, the teachings of the Chadwick reference and Hunt reference are inconsistent with these recited elements. Accordingly, the Applicant respectfully submits that Claims 1 and 17 are not obvious over Chadwick in view of Hunt, and are, therefore, allowable under 35 U.S.C. § 103(a). The Applicant respectfully requests that the rejection of Claims 1 and 17 be withdrawn.

There is no expectation of success.

In order to establish a prima facie case of obviousness based on a combination of references, there must be a reasonable expectation of success. For the reasons stated above, applicants respectfully submit that a person of ordinary skill in the art would have no reasonable expectation of success to modify Chadwick or to combine the teachings of Chadwick and Hunt to cure the deficiencies of Chadwick. Accordingly, the Applicant respectfully submits that Claims 1 and 17 are not obvious over Chadwick, either alone or in combination with Hunt, and are, therefore, allowable under 35 U.S.C. § 103(a). The Applicant respectfully requests that the rejection of Claims 1 and 17 be withdrawn.

The cited art does not teach or suggest all the claim elements.

Unless the reference(s) teach or suggest all the claim limitations, obviousness cannot be found. MPEP § 2143.03. Further, once an independent claim is found to be non-obvious under 35 U.S.C. § 103, then any claim which depends from that independent claim is also non-obvious. MPEP § 2143.03; In re Fine, 837 F.2d 1071 (Fed. Cir. 1988). For the reasons stated above, the Applicant respectfully submits that

the cited references do not disclose, teach or suggest all the claim elements of Claims 1 and 17. Accordingly, the Applicant respectfully submits that Claims 1 and 17 are not obvious over Chadwick, either alone or in combination with Hunt, and are, therefore, allowable under 35 U.S.C. § 103(a). The Applicant respectfully requests that the rejection of Claims 1 and 17 be withdrawn.

Claims 4-6 and 18

Because the Hunt reference, independently or in combination with the Chadwick reference, fails to anticipate or render obvious each and every element of the pending independent claims, the Applicant respectfully submits that independent Claims 1 and 17 and their respective dependent claims are in condition for allowance.

2.) Rejection under 35 U.S.C. 103(a) over "Merging and Extending the PDP and PEM Trust Models – The ICE-TEL Trust Model" in view of United States Patent No. 5,539,881 and further in view of United States Patent No. 6,691,173

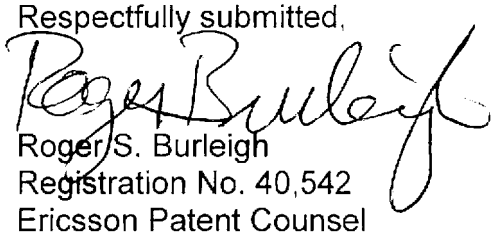
Claim 7-16 and 19-23

Because the Hunt reference, independently or in combination with Chadwick reference, fails to anticipate or render obvious each and every element of the pending independent claims, the Applicant respectfully submits that independent Claims 1 and 17 and their respective dependent claims are in condition for allowance. The Morris reference does not cure the deficiencies of the Chadwick reference or the Hunt reference.

CONCLUSION

The claims currently pending in the application are patentable over the cited references, and the Applicants request that the Examiner's rejection thereof be reversed and the application be remanded for further prosecution.

Respectfully submitted,



Roger S. Burleigh
Registration No. 40,542
Ericsson Patent Counsel

Date: July 24, 2006

Ericsson Inc.
6300 Legacy Drive, M/S EVR1 C-11
Plano, Texas 75024

(972) 583-5799
Roger.burleigh@ericsson.com

CLAIMS APPENDIX

1. A method for establishing security in an ad hoc communication network, the ad hoc communication network comprising a set of communication nodes, at least two nodes of the set of communication nodes having a mutual trust relation and comprising a trust group, the trust relations being created with public keys, and at least one additional node, the at least one additional node being a candidate node for joining the trust group within the ad hoc communication network, the nodes having authority to delegate trust to nodes of the set of communication nodes within the trust group, the method comprising the steps of:

receiving a request from the candidate node to join the trust group within said ad hoc communication network wherein said ad hoc communication network does not include a separate certificate authority;

identifying any node within the trust group having a trust relation with the candidate node, the node having the trust relation with the candidate node being an X-node; and

distributing trust relations between all members in the trust group

and the candidate node by means of the X-node distributing the public key associated with said candidate node to said all members of the trust group and wherein X-node further sending a signed message comprising a list of nodes that the X-node trusts within the ad hoc communication network and all corresponding public keys to the candidate node.

2-3. (Cancelled)

4. The method according to claim 1, wherein the distributing step comprises the X-node signing the candidate node's public key.

5. The method according to claim 4, wherein the distributing step comprises the X-node sending a message comprising the candidate node's signed public key to the nodes within the trust group.

6. The method according to claim 1, wherein the ad hoc communication network comprises a set of nodes comprising several trust groups, each of the set of nodes being candidates for joining all trust groups within the ad hoc communication network that the set of nodes are not already a member of, the method comprising, after receiving the messages, each node of the set of nodes creating a list of candidate nodes that a given node of the set of nodes trusts and corresponding public keys.

7. The method according to claim 6, further comprising deciding one node within the ad hoc communication network to act as a server node.

8. The method according to claim 7, further comprising the server node receiving, from each other node within the ad hoc communication network, a message comprising a respective public key, a respective list of candidate nodes that the respective node trusts, and corresponding public keys.

9. The method according to claim 8, further comprising the server node classifying the at least one candidate node as being a server-trusted node or as being a server-un-trusted node, depending on whether the server node trusts the at least one candidate node or not.

10. The method according to claim 9, wherein the identifying step further comprises the server node identifying at least one Y-node required for distributing trust relations between the server node and at least one server untrusted node.

11. The method according to claim 10, wherein said distributing step further comprises sending, by the server node, of a request to the identified at least one Y-node to distribute said trust relations between the server node and the server-untrusted nodes.

12. The method according to claim 11, wherein said distributing step further comprises obtaining, by the server node, of said requested trust relations.

13. The method according to claim 12, wherein the step of obtaining the trust relations further comprises:

signing, by the Y-node, of the public key of the server node for each server-untrusted node that the Y-node has a trust relation with; and

forwarding, by the Y-node, of said signed public key to the server-untrusted node.

14. The method according to claim 12, wherein the step of obtaining the trust relations comprises:

signing, by the Y-node, of the public key of the server-untrusted node for each server-untrusted node that the Y-node has a trust relation with; and

forwarding, by the Y-node, of said signed public key to the server node.

15. The method according to claim 12, comprising the further step of, after obtaining said trust relation, reclassifying, by the server node, the server-untrusted node with the obtained trust relation as being a server-trusted node.

16. The method according to claim 12, comprising the further step of sending, by the server node, of a signed message comprising the server node's trusted public keys belonging to trusted candidate nodes within the ad hoc communication network.

17. An ad hoc communication network comprising:

a set of communication nodes within said ad hoc communication network wherein said communication network does not have a separate certification authority,

each node of said set of communication nodes comprising a receiver and a computer, the computer comprising a processor and a memory, each node being interconnected with communication links, at least two of the nodes having a mutual trust relation and comprising a trust group, the trust relations being created with *public keys*,

at least one additional node of the set of communication nodes being a candidate node for joining at least one trust group within the ad hoc network,

the at least one candidate node having means for requesting if any of the nodes within the trust group have a trust relation with the candidate node, and

any one node being authorised to and having means for distributing trust relations between the trust group and the candidate node that the node trusts by distributing the public key associated with said candidate node to said nodes of the trust group and further distributing a list of nodes that the node trusts and all corresponding public keys to the candidate node.

18. The ad hoc communication network according to claim 17, wherein said each node comprises means for creating a list of candidate nodes that each node trusts and corresponding public keys of each node to be stored in the memory.

19. The ad hoc communication network according to claim 17, wherein one node of the set of communication nodes within the ad hoc network is operable as a server node capable of administrate distribution of trust relations.

20. The ad hoc communication network according to claim 19, wherein the server node is operable to classify the at least one candidate node as being a server-trusted node or as being a server-untrusted node, depending on whether the server node trusts the at least one candidate node or not.

21. The ad hoc communication network according to claim 20, wherein the server node comprises means for identifying at least one Y-node required for distributing trust relations between the server node and server-untrusted nodes.

22. The ad hoc communication network according to claim 21 , wherein the server node comprises means for sending to each of said at least one Y-node:

a request as to which of the server-untrusted nodes the Y-node has a trust relation with; and

a request for distributing trust relations between the server node and the requested server-untrusted nodes.

23. The ad hoc communication network according to claim 20, wherein the server node comprises means for distributing obtained trust relations to the nodes within the ad hoc communication network.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.